人工知能学会
第16回知識流通ネットワーク研究会
SIG-KSN-016-04

安全分析プロセスにおける D-Case の有効性

小林 展英
株式会社デンソークリエイト プロジェクトセンター
愛知県名古屋市中区栄 3-1-1

The effectiveness of D-Case in a safety analysis process

Nobuhide Kobayashi
Software Development Dept. Denso Create Inc.
3-1-1 Sakae Naka-Ku, Nagoya Aichi Japan

概要

ISO26262 対応を想定した安全分析では、安全性の分析結果だけでなく、その妥当性を第三者が納得する形で説明できることが求められている。本論文では、第三者が納得できる説明文書の作成において、HAZOP, FTA といった分析手法と D-Case を組み合わせることが有効であることを報告する。

Abstract

It's necessary to prepare not only the result of safety analysis, but also the enough explanation for stakeholders, in order to achieve ISO26262 compliance. In this paper, we introduce the effective method which combines D-Case with safety analysis methods HAZOP and FTA.

1. はじめに

安全性の高いシステムを開発するためには、HAZOP、FTA、FMEA といった分析手法を適切に組み合わせて漏れなくハザードを抽出し、その回避に必要な対策を決定する必要がある。さらに、システムの開発に携わっていない第三者がシステムの安全性を納得するためには、その対策が確実にシステムへ組込まれていることを説明できる必要がある。

本稿では、HAZOP などを用いて分析したハザードとその対策が、確実にシステムに組込まれていることを D-Case で説明する方法の有効性について考察する。2 章で今回採用した安全分析プロセスを説明する。3 章で本プロセスにおける D-Case の有効性を評価するために用いたシステムを示し、4 章でそのシステムに対して本プロセスを試行した結果を述べる。5 章では 4 章の結果に基づいた考察を述べ、6 章でまとめと今後の課題を明らかにする。

2. 今回採用した安全分析プロセス

本稿で採用した安全分析プロセスを以下に示す。次節以降で各工程の詳細について説明する。

① HAZOP を用いてシステムの外部視点からハザードを抽出する。
② FTA を用いてハザードの原因となる故障モードを抽出し、その回避に必要な対策を定義する。
③ D-Case を用いて故障モードの対策結果がシステムに組込まれていることを確認する。

なお、本稿では安全分析プロセスにおける D-Case の有効性評価に焦点を置くため、簡易的な分析方法を一部で採用している。

2.1. ハザード抽出

本工程では、HAZOP を用いてシステムのハザードを

抽出する。具体的には、システムが提供する機能の特性に応じてガイドワードを決定し、そのガイドワードに従って機能が正常動作から逸脱した状態をハザードとして抽出することとした。

2.2. 故障モード抽出と対策定義

本工程では、FTA を用いて抽出されたハザードの発生原因となる故障モードを抽出して必要な対策を定義する。具体的には、ハザードの発生に関連する装置をシステム構成図などから抽出し、さらにガイドワードを用いて装置毎に発生し得る故障モードを抽出することとした。故障モードを回避するための対策は、装置単体で回避できる場合には装置毎のスコープで対策を立案し、複数の装置に跨がった対策が必要な場合には、装置間共通の安全対策方針を定めた上で対策を立案することとした。

実際の開発においては、FTA と FMEA を併用して、トップダウン、ボトムアップの両面でハザードと故障モードの関係を分析した方が精度の高い分析が可能である。しかしながら、本稿では安全分析そのものではなく、D-Case を用いた分析結果の説明に焦点を置いているため、上述した簡易的な方法を採用している。

2.3. 故障モードの対策結果の確認

本工程では、第三者がシステムの安全性を確認できる説明文書を D-Case を用いて作成する。具体的には、第三者が説明文書を納得するために必要となる以下の 3 点について見える化する。

① 故障モードの抽出結果に納得できる
② 故障モードに対する対策に納得できる
③ 故障モードの対策がシステムに組込まれていることを確認できる

①については、故障モードを抽出した過程を、D-Case の説明ノードによる分解過程で表現し、分析時に用いた判断基準を前提ノードで表現する。②については、①と同様に対策立案に用いた判断基準を前提ノードで表現する。③については、前提ノードで表現した故障モードの対策と、証拠ノードで表現したシステムに対策を組込んだ記録の対応関係で表現することとした。

3. 安全分析プロセスの適用対象

本章では、安全分析プロセスにおける D-Case の有効性を評価するために使用したヘッドライト制御システムと、システムの中核を担うヘッドライト制御 ECU について説明する。なお、本稿では、安全分析プロセスにおける D-Case の有効性評価に焦点を置いている都合上、以下の点を省略している。

- システムを構成する装置（センサ、アクチュエータ、ECU）のハードウェア詳細
- 中核を担う ECU 以外のソフトウェア構成
- ECU に搭載されるソフトウェア部品の詳細

3.1. ヘッドライト制御システム

表 1 にヘッドライト制御システムが提供する機能、図 1 にシステムを構成する装置群（センサ、アクチュエータ、ECU）の関係を示す。

表 1 機能一覧

ID.	機能
1.	ユーザ操作に応じてヘッドライトを点灯
2.	ユーザ操作に応じてヘッドライトを消灯

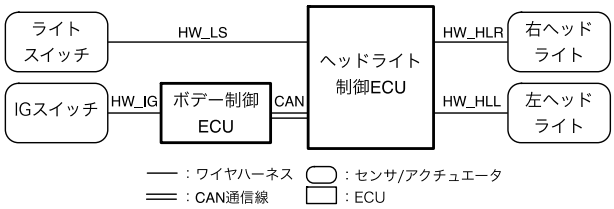

図 1 システム構成図

3.2. ヘッドライト制御 ECU

図 2 にヘッドライト制御 ECU に搭載されるソフトウェアの構成、およびヘッドライト制御 ECU の入出力とソフトウェア部品の関係を示す。

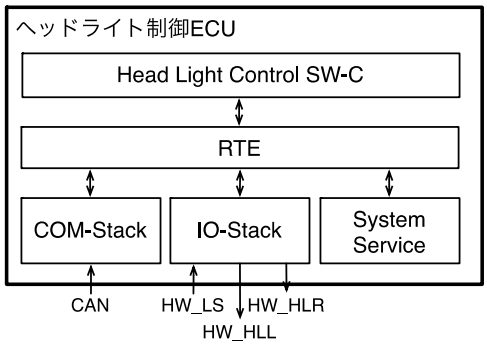

図 2 ECU ソフトウェア構成図

4. 安全分析プロセスの試行結果

本章では、2 章で定めた安全分析プロセスを用いて、3 章で示したヘッドライト制御システムの安全性を分析、および確認した結果を述べる。

4.1. ハザード抽出

ヘッドライトが持つ点灯、消灯という値に着目して“無し”、“異なる”、“過多”、“過少”をガイドワードとした。このガイドワードを用いて、表 1 に示した機能一覧を対象として HAZOP 分析した結果を表 2 に示す。なお、今回の試行では、ID.1 のみに絞って以降の工程を進めることとする。

表 2 ハザード分析結果

ID.	ガイドワード	ハザード
1.	無し	ヘッドライトの完全な喪失
2.	異なる	ユーザ操作に対するヘッドライトの点灯、消灯が逆転
3.	過多	ヘッドライトの光量が多い
4.	過少	ヘッドライトの光量不足

4.2. 故障モード抽出と対策定義

表 2 の ID.1 をトップ事象として、システム構成に従って故障モードを抽出した FTA 分析結果を図 4 に示す。故障モードに相当する FTA のリーフは、前述した表 2 と同じガイドワードを用いて抽出している。抽出した故障モードの対策は、以下に記す安全対策方針に基づき表 3 にまとめている。

【安全対策方針】

（方針１）走行中における突然のヘッドライト喪失を回避するため、ヘッドライト制御に関する故障検出時には点灯側で制御する。

（方針２）通信に関する途絶・誤り検出時には受信側で方針１に基づいて制御する。

4.3. 故障モードの対策結果の確認

「ヘッドライト制御システムは安全である」を D-Case のトップゴールとして、以下の順で説明を構造化した。

① システムの提供機能に対するハザード抽出結果
② システムを構成する装置の種別
③ 装置毎の故障モード抽出結果
④ 故障モードに対する対策箇所

さらに、上記④には、D-Case の証拠ノードに紐付けられた成果物が満足すべき基準として、故障モードの対策を前提ノードとして関連づけている。これにより、故障モードの対策がシステムに対して確実に組込まれていることを確認できるようにしている。上記をまとめた D-Case を図 5、図 6 に示す。

5. 考察

本章では、4 章の試行結果から気づきを得た D-Case の有効性と本プロセスの限界について考察する。

5.1. 本プロセスにおける D-Case の有効性

5.1.1. 安全分析の全体像の見える化

第三者にシステムの安全性を納得してもらうためには、安全分析の進め方の全体像が俯瞰できるビューが必要である。今回の試行では、ハザード分析、故障モード分析、対策立案、の順に安全分析を進めているが、その順に従って D-Case の階層構造を決定したことで、安全分析の進め方を第三者が全体俯瞰できるビューを提供することができている。それに加えて、分析に用いた方針やガイドワードなどの判断基準も前提ノードで見える化できるため、第三者に全体俯瞰させるビューとして D-Case は有効であると言える。

5.1.2. 安全対策方針の記述品質の見える化

安全対策方針が適切なスコープで定義されていることは、システムを構成する要素間の振舞いの整合性を確保する上で不可欠である。例えば、図 3 中の C1 は大方針として必要であるが、この抽象度の方針のみで安全対策を進めた場合、システムの構成要素毎に異なる解釈をして対策間に不整合が生じ、システム全体として安全性が確保できなくなる恐れがある。D-Case を用いて安全分析の結果を構造化したことで、スコープの特性に応じて C1 の方針を具体化した C2 のような方針が、他と矛盾のない表現、かつ適切なスコープ

で配置されているか容易に確認することができる。このことから、構成要素間の不整合検出に不可欠な安全対策方針の記述品質の判断に有効であると言える。

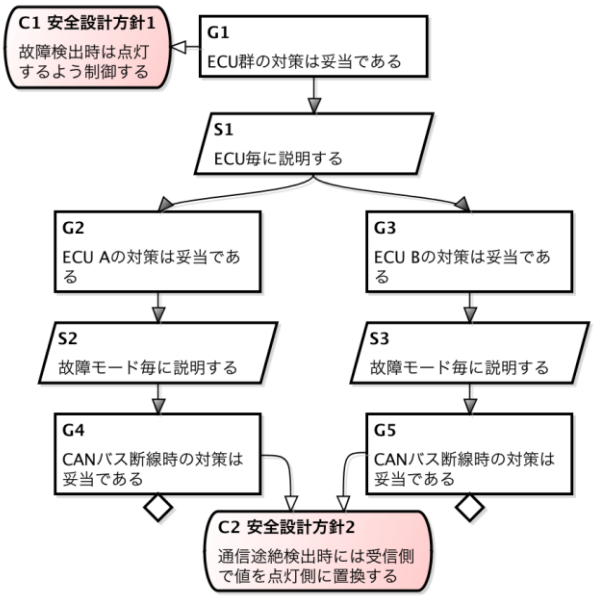

図 3 安全対策方針の記述品質の見える化

5.1.3. システムへの組込み状況の見える化

2.3 節の③で定めた通り、故障モードの対策を前提ノードに紐付け、それを満足できる記録を証拠ノードに紐付けるルールで D-Case を作成した結果、対策の組込み状況を前述した２つのノードの対応関係のみで確認できることが実証できた。実際の開発では、システムに組込む対策が決定してから多くの設計工程を経た上でシステムに組込まれることになり、その変換過程の記録を目的としたトレーサビリティマトリクスには、設計視点で変換過程が記録されている。このため、安全分析の視点に絞って確認するビューとして必ずしも最適ではない場合がある。一方、D-Case をビューに用いた場合、5.1.1 節で述べたように第三者への説明に必要な情報としてハザードから故障モードの抽出、さらにその対策定義までの過程が見える化されている。また、FTA の表記法だけでは見える化が難しい組込み状況を確認した記録との対応付けも容易であり、第三者が確認するビューとして有効であると言える。

5.2. 本プロセスの限界

故障モードの対策定義に際しては、該当する故障モードの重要性などを分析して必要十分な対策を定義する必要がある。本稿で採用したプロセスを実際の開発現場で運用する場合、上述した工程の追加が必要である。

6. まとめと今後の課題

本稿では、第三者による安全性の確認で必要となる、全体俯瞰、判断基準、対策の組込み状況の見える化に対して、HAZOP, FTA の分析結果を前提として D-Case を作成することが有効であることを確認できた。実際の開発現場での運用を想定すると、D-Case 形式での確認は表記ルールを理解していない相手にはハードルが高いこともあり、自然言語形式の文書を期待される可能が高い。この点を踏まえると、確認に用いる文書の初版を D-Case 形式で作成し、それに基づいて自然言語形式の文書を作成する流れが現場運用では最良であるように考えている。今後の課題としては、上記仮説を実証するために、D-Case の導入有無で確認に用いる文書の納得度や生産性に影響があるか実験に取り組んでいきたい。

謝辞

本稿執筆に当たってご指導頂いた名古屋大学山本修一郎先生、ならびに試行データ作成に協力頂いた社員の皆様に感謝します。

参考文献

[1] 実践D-Case , 松野裕, 山本修一郎, 株式会社アセットマネジメント, 2013
[2] 議論パターンポケットガイド アルファ版, 山本修一郎, 名古屋大学, 2014
[3] DEOS 変化しつづけるためのディペンダビリティ工学, 所眞理雄, 近代科学社, 2014
[4] ISO26262 実践ガイドブック入門編, ビジネスキューブ・アンド・パートナーズ, 日経 BP 社, 2012
[5] ボッシュ自動車ハンドブック, ロバートボッシュ GmbH 著, 株式会社シュタールジャパン, 2011

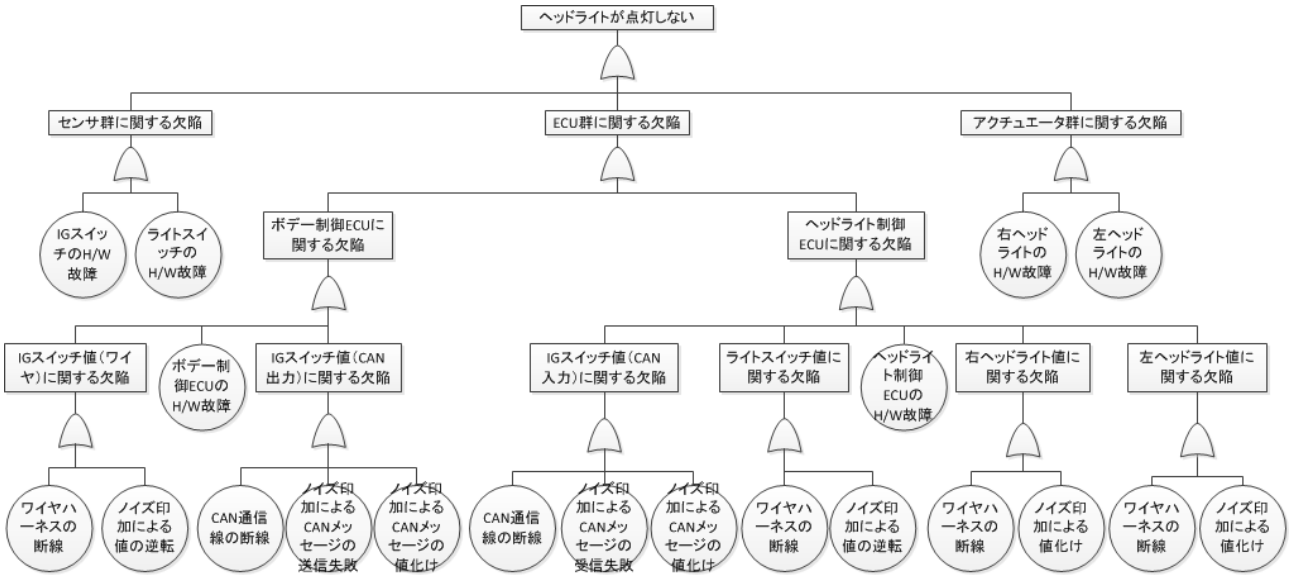

図 4 FTA を用いた故障モードの分析結果

表 3 故障モードの分析結果に対する対策（ECU 群のみ）

ID.	システム要素	故障モード	対策
1.	ボデー制御 ECU	IG スイッチ値のワイヤハーネス断線	H/W 回路で断線時の値をオンとする
2.		ノイズ印可による IG スイッチ値の逆転	IO-Stack で IG スイッチ値のチャタリングを防止する
3.		ボデー制御 ECU の H/W 故障	ヘッドライト制御 ECU 側で対応する
4.		CAN 通信線断線	〃
5.		ノイズ印可による CAN メッセージ送信失敗	〃
6.		ノイズ印可による CAN メッセージの値化け	COM-Stack で誤り検出符号を付与する
7.	ヘッドライト制御 ECU	CAN 通信線断線	COM-Stack で通信途絶時の IG スイッチ値をオンとする
8.		ノイズ印可による CAN メッセージ受信失敗	〃
9.		ノイズ印可による CAN メッセージの値化け	COM-Stack で誤り検出時の IG スイッチ値をオンとする
10.		ライトスイッチ値のワイヤハーネス断線	H/W 回路で断線時の値をオンとする
11.		ノイズ印可によるライトスイッチ値の逆転	IO-Stack でライトスイッチ値のチャタリングを防止する
12.		ヘッドライト制御 ECU の H/W 故障	別システムで故障監視してダイアグ記録する
13.		右ヘッドライト値のワイヤハーネス断線	右ヘッドライト側で対応する
14.		ノイズ印可による右ヘッドライト値の値化け	〃
15.		左ヘッドライト値のワイヤハーネス断線	左ヘッドライト側で対応する
16.		ノイズ印可による左ヘッドライト値の値化け	〃

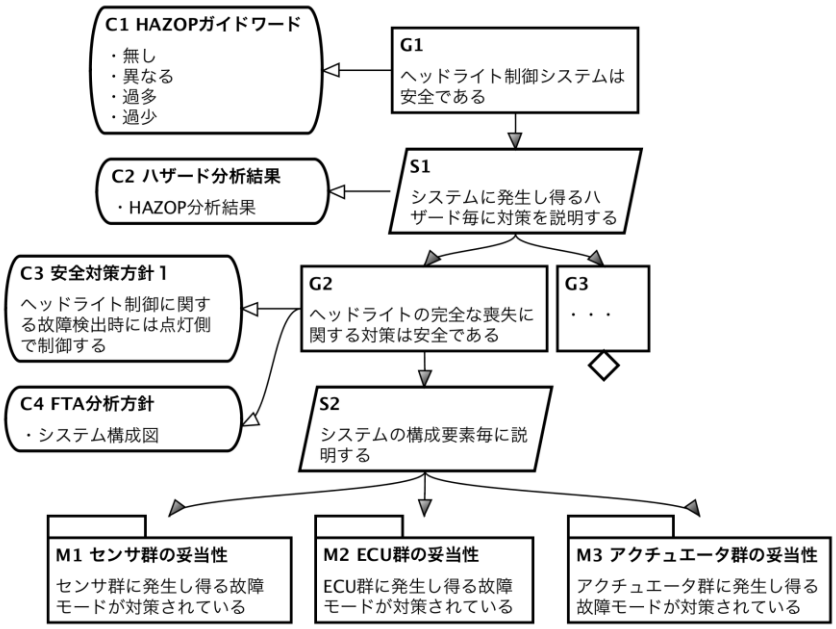

図 5 安全分析結果の説明（全体）

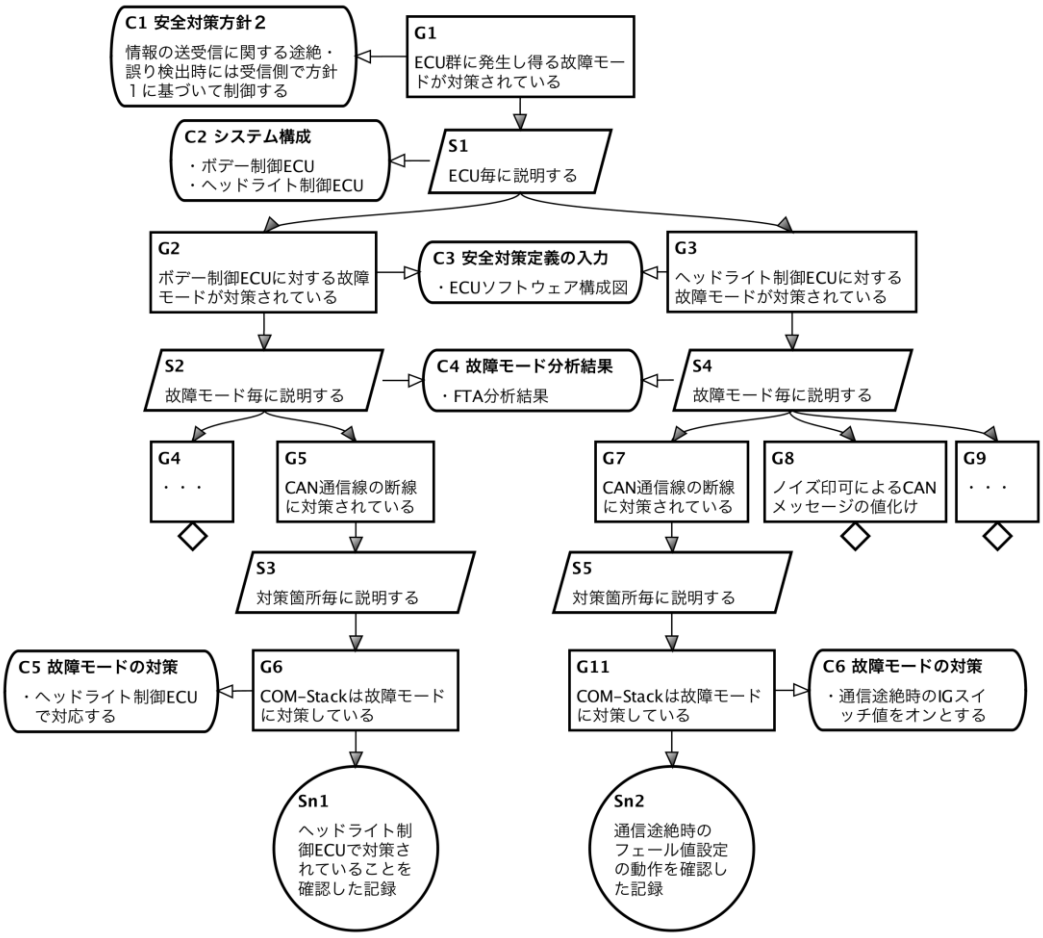

図 6 安全分析結果の説明（ECU 群の妥当性の抜粋）